REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
29/03/2017	Final	01/01/2013-12/31/2016

4. TITLE AND SUBTITLE
Investigation on Covert Channel Attacks and Countermeasures in the Cloud

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-13-1-0088

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Haining Wang

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
College of William and Mary

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Information security and privacy in general are major concerns that impede enterprise adaptation of shared or public cloud computing. Specifically, the concern of virtual machine (VM) physical co-residency stems from the threat that hostile tenants can leverage various forms of side channels (such as cache covert channels) to exfiltrate sensitive information of victims on the same physical system. Understanding attack strategies is the first step to stay ahead of the game and continue improving our security systems. Thus, investigating novel attack strategies and tactics is crucial to shaping the future directions of defense systems in the cloud. The objective of this project is to offer insightful analysis and effective defenses.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Haining Wang
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	U		757-813-4390

Final Report for

"Investigation on Covert Channel Attacks and Countermeasures in the Cloud"

Haining Wang

Adjunct Professor
Department of Computer Science
College of William and Mary
P.O. Box 8795
Williamsburg, VA 23187-8795
Email: hnw@cs.wm.edu
Phone: 757-813-4390
Fax: 757-221-1717

1 Overall Technical Achievement

Information security and privacy in general are major concerns that impede enterprise adaptation of shared or public cloud computing. Specifically, the concern of virtual machine (VM) physical co-residency stems from the threat that hostile tenants can leverage various forms of covert channels to exfiltrate sensitive information of victims on the same physical system. Understanding attack strategies is the first step to stay ahead of the game and continue improving our security systems. Thus, investigating novel attack strategies and tactics is crucial to shaping the future directions of defense systems in the cloud. The main contribution of this project is on revealing unknown vulnerabilities in a virtualized environment and developing effective countermeasures to thwart the new covert channel attacks in the cloud. Overall, the major technical achievements of this project includes:

- We have proposed and built new covert channel attacks, which are high-bandwidth and reliable for data exfiltration. We have demonstrated the feasibilities of the proposed attacks and measure their damages through testbed and real experiments.
- We have proposed a series of defense mechanisms to effectively foil the new covert channel attacks in the cloud. In particular, considering the virtualized environments inside the cloud, we have developed the countermeasures from three different aspects: tenants, cloud service vendors, and the hardware device manufactures.
- We have investigated how VM placement policies inside the cloud could affect the construction of a covert channel and the corresponding defense against it. We have conducted a

systematic measurement study on the evolution of VM placement inside the cloud of Amazon EC2.

- We have quantified the easiness of mounting a co-residence attack inside the cloud. We have compared our results with those of previous works, and then have made an attempt to understand how EC2 have adjusted their VM placement policies.

The success of this project offers insightful analysis and effective countermeasures for next-generation covert channel attacks in the cloud. We believe that the results of this project will enable transformative rethinking of the current information security and privacy issues in the cloud beyond traditional detection and prevention techniques.

2 Description of the Specific Problems

In this project, leveraging our successful experience in covert channels research, we will investigate novel covert channel attack techniques in the cloud, and seek the corresponding countermeasures. In the first part of this project, we plan to show that the threat of covert channel attacks in the cloud is real and practical. We will first study existing cache covert channel techniques and their applications in a virtualized environment. In our preliminary study, we have revealed that these techniques are rendered ineffective by virtualization, due to three major insufficiency and difficulties, namely, addressing uncertainty, scheduling uncertainty, and cache physical limitations. We will tackle the addressing and scheduling uncertainty problems by designing a new data transmission scheme with relaxed dependencies on precise cache line addressing and scheduling patterns. Then, we will overcome the cache physical limitations by discovering a high-bandwidth memory bus covert channel, exploiting the atomic instructions and their induced cache–memory bus interactions on x86 platforms.

3 Description for the Approach Taken

The classic cache channels work very well on hyper-threaded systems, achieving transmission rates as high as hundreds of kilobytes per second. However, when applied in todays virtualized environments, the achievable rates drop drastically, to only low single-digit bits per second. The multiple orders of magnitude reduction in channel capacity clearly indicates that the classic cache channel techniques are no longer suitable for cross-VM data transmission. In this project, we have found that on virtualized platforms, the data transmission scheme of a classic cache channel suffers three major obstaclesaddressing uncertainty, scheduling uncertainty, and cache physical limitation.

To tackle the existing difficulties and develop a high-bandwidth, reliable covert channel on virtualized x86 systems, we have first developed our redesigned, pure timing-based data transmission scheme, which overcomes the negative effects of addressing and scheduling uncertainties with a simplified design. Then, we have found a powerful covert channel medium by exploiting the atomic instructions and their induced cachememory bus interactions on x86 platforms. And finally, we have tuned our designs of a high error-tolerance transmission protocol for cross-VM covert channels. Our evaluation methodology is the combination of testbed based experiments and real-world implementation and deployment. In particular, we have evaluated the exploitability

of memory bus covert channels by implementing the reliable Cross-VM communication protocol, and have demonstrated covert channel attacks and their countermeasures on our in-house testbed server, as well as on the Amazon EC2 cloud.

3.1 Advantages of the Approach

- We first had a deep understanding on existing cache-based covert channels, and reveal why they do not work well in a cloud environment.
- We then developed a novel timing-based covert channel, instead of following the conventional cache-region-based approaches, to achieve high-bandwidth and reliable cross-VM communications.
- We exploited a new medium, such as memory bus or memory deduplication, to overcome the physical limitation in sharing resources and construct a more reliable covert channel.
- We developed effective and low-cost defense mechanisms against data exfiltration attacks inside the cloud, including controlled and deterministic resource sharing as well as resource isolation improvements.

4 Key Outcomes

The project started in January, 2013, and has supported five Ph.D. students for their security and system research in the cloud. As scheduled, we have systematically developed the proposed covert channel attacks and explored new vulnerability in the cloud, especially from the power and energy perspectives, as well as corresponding countermeasures against these attacks. We have published three journal papers and 15 conference papers in ACM CCS, IEEE S&P, USENIX Security, NDSS, WWW, ACM MMSys, RAID, IEEE ICNP, CODASPY, IEEE DSN, ESORICS, and SecureComm.

- Xin Ruan, Zhenyu Wu, Haining Wang, and Sushil Jajodia, "Profiling Online Social Behaviors for Compromised Account Detection", In *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 1, January 2016.
- Zhenyu Wu, Zhang Xu, and Haining Wang, "Whispers in the Hyper-space: High-bandwidth and Reliable Covert Channel Attacks inside the Cloud", In *IEEE/ACM Transactions on Networking (ToN)*, Vol. 23, No. 2, April 2015.
- Zhenyu Wu, Yueping Zhang, Vishal K. Singh, Guofei Jiang, and Haining Wang, "Automating Cloud Network Optimization and Evolution", In *IEEE Journal on Selected Areas in Communications (JSAC)*, Special Issue on Networking Challenges in Cloud Computing Systems and Applications, December 2013.
- Daiping Liu, Shuai Hao, and Haining Wang, "All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records", In *Proceedings of ACM CCS 2016*, Vienna, Austria, October 2016.

- Zhang Xu, Zhenyu Wu, Zhichun Li, K. Jee, J. Rhee, X. Xiao, F. Xu, Haining Wang, and Guofei Jiang, "High Fidelity Data Reduction for Big Data Security Dependency Analyses", In *Proceedings of ACM CCS 2016*, Vienna, Austria, October 2016.

- Aaron Koehl and Haining Wang, "SERF: Optimization of Socially Sourced Images using Psychovisual Enhancements", In *Proceedings of ACM Multimedia Systems (MMSys) 2016*, Klagenfurt, Austria, May 2016.

- Shuai Hao, Haining Wang, Angelos Stavrou, and Evgenia Smirni, "On the DNS Deployment of Modern Web Services", In *Proceedings of IEEE ICNP 2015*, San Francisco, CA, November 2015.

- Haitao Xu, Haining Wang, and Angelos Stavrou, "Privacy Risk Assessment on Online Photos", In *Proceedings of RAID 2015*, Kyoto, Japan, November 2015.

- Jidong Xiao, Hai Huang, and Haining Wang, "Defeating Kernel Driver Purifier", In *Proceedings of SECURECOMM 2015*, Dallas, TX, October 2015.

- Zhang Xu, Haining Wang, and Zhenyu Wu "A Measurement Study on Co-residence Threat inside the Cloud", In *Proceedings of USENIX Security Symposium 2015*, Washington, D.C., August 2015.

- Haitao Xu, Daiping Liu, Haining Wang, and Angelos Stavrou, "E-commerce Reputation Manipulation: The Emergence of Reputation-Escalation-as-a-Service", In *Proceedings of WWW 2015*, Florence, Italy, May 2015.

- Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun, "Using Hardware Features for Increased Debugging Transparency", In *IEEE Symposium on Security and Privacy (S&P) 2015*, San Jose, CA, May 2015.

- Zhang Xu, Haining Wang, Zichen Xu, and Xiaorui Wang, "Power Attack: An Increasing Threat to Data Centers," In Proceedings of Network and Distributed System Security (NDSS) Symposium 2014, San Diego, CA, February 2014.

- Hemant Sengar, Haining Wang, and Seyed Amir Iranmanesh, "Wiretap-proof: What They Hear is Not What You Speak, and What You Speak They Do Not Hear," In Proceedings of ACM CODASPY 2014, San Antonio, TX, March 2014.

- Daiping Liu, Haining Wang, and Angelos Stavrou, "Detecting Malicious Javascript in PDF through Document Instrumentation," In Proceedings of IEEE DSN 2014, Atlanta, GA, June 2014.

- Fengwei Zhang, Haining Wang, Kevin Leach, and Angelos Stavrou, "A Framework to Secure Peripherals at Runtime ," In Proceedings of ESORICS 2014, Wroclaw, Poland, September 2014.

- Haitao Xu, Daiping Liu, Aaron Koehl, Haining Wang, Angelos Stavrou, "Click Fraud Detection on the Advertiser Side," In Proceedings of ESORICS 2014, Wroclaw, Poland, September 2014.

- Jidong Xiao, Zhang Xu, Hai Huang, and Haining Wang, "Security Implications of Memory Deduplication in a Virtualized Environment", In *Proceedings of IEEE DSN 2013*, Budapest, Hungary, June 2013.

4.1 Paper Awards

- Best Paper Award, USENIX LISA 2015.
- Best Paper Nominee, WWW 2015.
- Best Paper Nominee, IEEE ICNP 2015.

4.2 Graduated Ph.D. Students

- Aaron Koehl, May 2015
- Haitao Xu, December 2015
- Jidong Xiao, December 2015
- Zhang Xu, April 2016
- Xin Yuan, December 2016